UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/584,193	02/23/2007	Takehiro Ohkoshi	2565-0296PUS1	1279

2292   7590   12/24/2008
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER
SQUIRES, BRETT S

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
12/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _23 February 2007_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-6_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) _5_ is/are allowed.

6)☒ Claim(s) _1-4_ is/are rejected.

7)☒ Claim(s) _6_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _23 June 2006_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _06/23/06, 09/27/06, 02/23/07_.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Claim Objections

1.   Claim 3 is objected to because of the following informalities: claim 3 recites "an authenticated device," on page 22 line 4 and "an authenticated device," on page 22 line 8 it is unclear whether the recited claim limitations are intended to refer to different authenticated devices. Appropriate correction is required.

2.   Claim 6 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 5. The naming convention used for the steps in claim 5 does not provide any acts to distinguish the method of claim 5 from the method of claim 6. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5.   Claim 3 recites the limitation "the authenticating device" in page 22 line 10. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

6.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-4 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-4 recite "an authenticating device," and "an authenticated device," comprised of various different units. The preferred embodiments of the authenticating device and the authenticated device , disclosed in page 20 lines 1-5, discloses the units include software modules. Therefore, the claimed authenticating device and authenticated device are drawn to functional descriptive material and does not fall into at least one of the four statutory classes defined by 35 U.S.C. 101. If a claim covers material not found in any of those four categories, then the claim falls outside the plainly expressed scope of 35 U.S.C. 101, even if the subject matter is otherwise new and useful. *See In re Nuijten 84 USPQ2d 1495 (Fed. Cir. 2007)*

Claim Rejections - 35 USC § 102

7.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8.   Claims 1 and 3 are rejected under 35 U.S.C. 102(e) as being anticipated by Yeh

et al. (US 2005/0120203).

        Yeh discloses an authenticating device ("Authentication Server" See fig. 1 ref. no.

10) having an authentication processing unit ("Processor" and "Memory" See figs. 2-3

ref. no. 136 and138) to perform an authentication process with an authenticated device

("Client Device" See fig. 1 ref. no. 20) using an authentication key ("The authentication

server transmits a signed certificate to client device." See paragraph 11), an update key

generating unit ("Processor" "Memory" and "Automatic Rekey" See figs. 2-3 ref. nos.

136, 138, 260 and paragraphs 48-51)to generate a new authentication key when the

authenticated device does not hold an authentication key to be used in the

authentication process by the authentication processing unit ("The client device fails to

verify the signed certificate with the current public key and in response to the failure

requests an update public key from the authentication server." See paragraphs 11-13

The examiner respectfully points out that when the client device does not hold a public

key the client device will also fail to verify the signed certificate and in response to the

failure will request an update public key from the authentication server.), and to

generate a new authentication key for updating an authentication key to be used in the

authentication process by the authentication processing unit when the authenticated

device holds the authentication key but the authentication process with the

authentication device by the authentication processing unit fails ("The client device fails

to verify the signed certificate with the current public key and in response to the fail

requests an update public key from the authentication server." See paragraphs 11-13),

wherein the authentication processing unit performs the authentication process with the

authenticated device again using the new authentication key generated by the update

key generating unit ("The client the uses the new public key for future authentication of

the server, for example, by replacing the current public key of the client with the new,

updated, public key." See paragraph 53).

Regarding Claim 3:

     Yeh discloses an authenticated device ("Client Device" See fig. 1 ref. no. 20)

having a memory unit ("Memory" See figs. 2-3 ref. no. 136 and138) to store a

prescribed algorithm identifier and a prescribed encryption key identifier, an

authentication processing unit ("Processor" and "Memory" See figs. 2-3 ref. no. 136

and138) to perform an authentication process with an authenticating device

("Authentication Server" See fig. 1 ref. no. 10) using an authentication key ("The client

device receives a signed certificate from the server and attempts to verify the signed

certificate with the current public key" See paragraph 11), a transmitting unit ("I/O Data

Ports" See fig. 2 ref. no. 146 and paragraph 48) to transmit the prescribed algorithm

identifier and the prescribed encryption key identifier stored by the memory unit to the

authenticating device when the authentication process with the authenticating device by

the authentication processing unit fails ("The client automatically updates the public key

associated with the server with an updated public key responsive to detecting failure of

authentication with the client's current public key." See paragraph 11), a receiving unit

("I/O Data Ports" See fig. 2 ref. no. 146 and paragraph 48) to receive from the

authenticating device a new authentication key based on the prescribed algorithm

identifier and the prescribed encryption key identifier transmitted by the transmitting unit,

and wherein the authentication processing unit performs the authentication process with

the authenticating device again using the new authentication key received by the

receiving unit ("The client the uses the new public key for future authentication of the

server, for example, by replacing the current public key of the client with the new,

updated, public key." See paragraph 53).

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

10.   Claims 2 and 4 are rejected under 35 U.S.C. 103(a) as being obvious over Yeh

et al. (US 2005/0120203) in view of Edgett et al. (US 2004/0034771).

Regarding Claim 2:

Yeh discloses the above stated authenticating device ("Authentication Server"

See fig. 1 ref. no. 10) having a receiving unit ("I/O Data Ports" See fig. 2 ref. no. 146 and

paragraph 48) to receive a prescribed algorithm identifier and a prescribed encryption

key identifier from the authenticated device ("The request includes an identification of

the current public key." See paragraph 13), a transmitting unit transmit ("I/O Data Ports"

See fig. 2 ref. no. 146 and paragraph 48) the new authentication key generated by the

update key generating unit to the authenticated device ("The client device receives the

updated public key over a connection from the authentication server." See paragraph
12), and wherein the authentication processing unit performs the authentication process
with the authenticated device again using the new authentication key transmitted by the
transmitting unit ("The client the uses the new public key for future authentication of the
server, for example, by replacing the current public key of the client with the new,
updated, public key." See paragraph 53).

Yeh does not disclose the update key generating unit generates the new
authentication key based on the prescribed algorithm identifier and the prescribed
encryption key identifier received by the receiving unit.

Edgett discloses a system for changing security information in a computer
network having an ISP authentication system (See fig. 1 ref. no. 18) that receives a key
index for a public/private key pair as well as an algorithm identifier (See paragraph 58)
and uses the key index and the algorithm identifier to determine when the validity
periods for the public/private key pair and the encryption algorithm have expired (See
paragraph 49). The ISP authentication system generates a new public/private key pair
and encryption algorithm based on the key index and algorithm identifier identifying an
expired public/private key pair and an expired encryption algorithm (See paragraph 49).

It would have been obvious to one of ordinary skill in the art at the time of the
invention to modify the authenticating device disclosed by Yeh to include generating the
new authentication key based on a key index and an algorithm identifier such as that
taught by Edgett in order to reduce the likelihood that an intended user may be spoofed

by replacing algorithms with known weaknesses and the keys that have been generated

with the weak algorithms (See Edgett paragraphs 3 and 57).

Regarding Claim 4:

Yeh discloses an authenticated device having a receiving unit that receives

prescribed information from the authentication device when the authentication process

with the authentication device by the authentication processing unit fails ("The client

device receives a signed certificate from the authentication server." See paragraph 11)

and a transmitting unit that transmits a prescribed encryption key identifier stored by the

memory unit when the prescribed information has been received by the receiving unit

("The request for an updated public key includes an identification of a current public of

the client device" See paragraph 17).

Yeh does not disclose the transmitting unit transmits a prescribed algorithm

identifier stored by the memory unit when the prescribed information has been received

by the receiving unit.

Edgett discloses a system for changing security information in a computer

network having a networking accessing device (See fig. 1 ref. no. 34) that transmits a

key index for a public/private key pair as well as an algorithm identifier (See paragraph

58) to an ISP authentication system (See paragraph 58).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the authenticating device disclosed by Yeh to include transmitting a

key index and an algorithm identifier to the authentication server such as that taught by

Edgett in order to reduce the likelihood that an intended user may be spoofed by

replacing algorithms with known weaknesses and the keys that have been generated

with the weak algorithms (See Edgett paragraphs 3 and 57).

Allowable Subject Matter

11.   Claim 5 is allowed over the prior art of record. The combination of transmitting

steps, receiving steps, generating step, key updating step, and confirmation steps

performed by the key update method recited by claim 5 is not found in the prior art of

record. Further, there is insufficient motivation to combine the different steps performed

key update method if the different steps were found in separate prior art teachings.

Conclusion

12.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to BRETT SQUIRES whose telephone number is (571)

272-8021. The examiner can normally be reached on 9:30am - 6:00pm Monday -

Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/Christopher A. Revak/
Primary Examiner, Art Unit 2431